Cybersecurity Best Practices

Cybersecurity threats continue to grow in sophistication and frequency. While Nvest employs robust internal security controls and processes to safeguard your information, **cybersecurity is a shared responsibility**. Your daily habits play a critical role in keeping your personal and financial data secure.

Please review and apply the following best practices in your everyday digital life.

Securely Stored Strong Passwords

Poorly chosen passwords are quickly hacked. Don't put yourself at risk!

- Passwords should be at least 15 characters and consist of a combination of upper- and lower-case letters, numbers, and symbols.
- Use different passwords for each application (your email address, websites, mobile banking, Nvest client portal, and other applications).
- Always store passwords securely in a password vault app – not a sticky note on your refrigerator! For information on a good password vault, feel free to contact us.
- Enable multi-factor authentication – this may seem like a pain, but it is an added layer of protection.

Secure Your Mobile Devices

Mobile devices like your phone or tablet pose unique security risks.

- Check for software updates regularly and when available run updates promptly.
- Lock your phone number with your cellular provider, so a scammer can't "port" your number away from you.
- Consider installing a Virtual Private Network (VPN) for enhanced security and turn it on when using public Wi-Fi.

Be Aware of Phishing Scams

Phishing is when cybercriminals pose as trustworthy to lure you into providing sensitive information so to gain access to accounts and personal files.

- Unexpected requests through email or text messages asking you to verify sensitive information like a credit card number, social security number or account password are likely a scam. Do not respond or click links and attachments!
- Messages that create a sense of urgency and demand your immediate response, threaten criminal consequences, contain poor grammar and spelling mistakes are most likely a scam. Do not respond or click links and attachments!
- If you hover over a link within an email with your cursor and the URL doesn't match the description of the link, it might be malicious. Do not click it!

Verify Callers

If you can't verify the caller's identity you've likely spotted a scammer.

- Don't answer unknown numbers. If you do answer and it's a recording or someone pressuring you to take action, hang up.
- The caller claims to be from a Fraud Department. While your bank may contact you if it suspects fraudulent transactions, they already know who you are and will not ask you to verify account numbers, etc. Hang up and call the financial institution with the number you already have.
- Be wary of answering questions – even seemingly harmless ones like "what is your name" or repeat phrases like "yes" or "no." Scammers may be attempting to capture a recording of your voice to generate an AI copy.

Need guidance? We're here to help you build information security confidence. Call us at 207-985-8585 or email info@nvestfinancial.com.

*Source: CISA.gov (Cybersecurity & Infrastructure Security Agency)

All information has been obtained from sources believed to be reliable, but its accuracy is not guaranteed. There is no representation or warranty as to the current accuracy, reliability or completeness of, nor liability for, decisions based on such information, and it should not be relied on as such.

Version 1/8/2026